(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 001 640 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
17.05.2000 Patentblatt 2000/20

(51) Int. Cl.[7]: **H04Q 7/32**

(21) Anmeldenummer: **99121688.8**

(22) Anmeldetag: **02.11.1999**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **16.11.1998 DE 19852732**

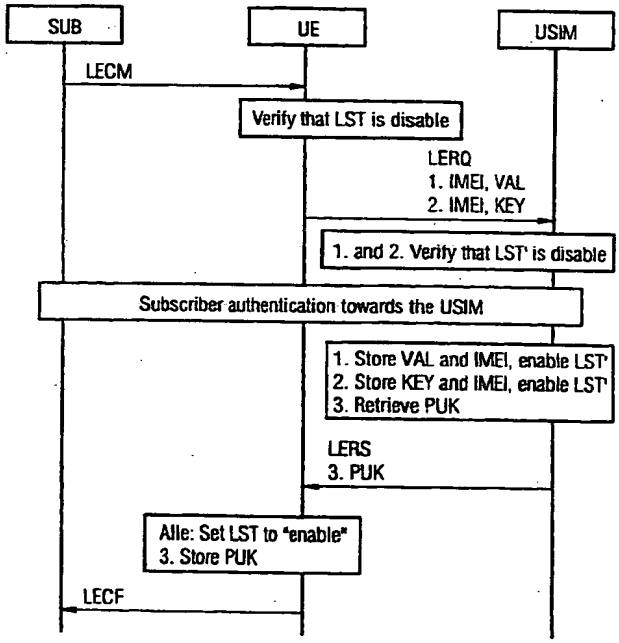
(71) Anmelder:
SIEMENS AKTIENGESELLSCHAFT
80333 München (DE)

(72) Erfinder: **Vinck, Bart**
2050 Antwerpen (BE)

(54) Sicherung von Mobilstationen eines Funk-Kommunikationssystems

(57) Ausgehend davon, dass jede Mobilstation (MT) ein Identitätsmodul (USIM) und eine Benutzergerät (UE) aufweist, wird gemäß dem Gegenstand der Erfindung das Benutzergerät (UE) durch ein teilnehmergesteuertes Sperren und Entsperren gegen einen Missbrauch gesichert. Das erfindungsgemäße Merkmal, teilnehmergesteuert ein Sperren/Entsperren des Benutzergeräts (UE) durchzuführen, macht vorteilhafterweise ein netzseitiges zentrales Register mit Gerätekennungen zur Identifikation gestohlener Benutzergeräte redundant und erhöht für den Teilnehmer somit den Grad der Sicherheit der von ihm verwalteten Benutzergeräte.

FIG 2



EP 1 001 640 A1

SUB. Bei erfolgreicher Authentifikation bestätigt das Identitätsmodul USIM das Entsperren des Benutzergeräts UE, wobei es zuvor ihren entsprechenden Zustand LST' für das Benutzergerät UE intern zurücksetzt (LST' disabled) - siehe FIG 4. Zur Bestätigung sendet es eine Nachricht LDRS (Lock Disable Response) zurück, woraufhin die Steuereinrichtung CU das Aufheben der bisherigen Sperre in der Speichereinrichtung MU (LST disabled) veranlaßt und das Entsperren dem Teilnehmer SUB mit der Nachricht LDCF (Lock Disable Confirm) bestätigt - siehe FIG 4.

[0015] Wenn erfindungsgemäß die Sperre im Benutzergerät US aufgehoben ist, erkennbar am Zustand LST, hat jeder Teilnehmer SUB die Möglichkeit die Sperre wieder einzuschalten und das Benutzergerät UE an die Chipkarte UICC mit seinem Indentitätsmodul USIM zu binden. Der Teilnehmer SUB gibt einen entsprechenden Befehl LECM (Lock Enable Command) ein - siehe FIG 2 - , der von der Steuereinrichtung CU des Benutzergeräts US in eine Nachricht LERQ (Lock Enable Request) umgesetzt und zum Identitätsmodul USIM dann ausgesendet wird, wenn der Zustand LST dies erlaubt (LST disabled). Die erforderlichen Schitte veranlasst die Steuereinrichtung CU.. Das Identitätsmodul USIM authentifiziert dann den Teilnehmer SUB. Bei erfolgreicher Authentifikatlon bestätigt das Identitätsmodul USIM das Sperren des Benutzergeräts UE, wobei es zuvor ihren entsprechenden Zustand LST' für das Benutzergerät UE intern setzt (enable LST') - siehe FIG 2. Zur Bestätigung sendet es eine Nachricht LERS (Look Enable Response) zurück, woraufhin die Steuereinrichtung CU das erneute Setzen der Sperre in der Speichereinrichtung MU (LST enabled) veranlaßt und den gesperrten Zustand dem Teilnehmer SUB mit der Nachricht LECF (Lock Enable Confirm) bestätigt - siehe FIG 2.

[0016] Die Teilnehmerauthentifikation ist vorzugsweise sowohl beim Sperren als auch beim Entsperren erforderlich. Dabei finden bevorzugt andere Sicherheitsparameter Anwendung als die bei einer Benutzerauthentifikation zur Überprüfung der Zugangsberechtigung des mobilen Benutzers zum Funk-Kommunikationssystem benutzten Sicherheitsparameter. Im einfachsten Fall wird zur Teilnehmer- und Benutzerauthentifikation eine persönliche Identifikationsnummer verwendet, die für den Teilnehmer SUB aus der Nummer SPIN und für den Benutzer USE aus der Nummer UPIN besteht.

[0017] Die Zustände Sperren/Entsperren für das Benutzergerät UE sind durch das Identitätsmodul USIM änderbar, jeweils auf Anforderung eines Teilnehmers oder Benutzers der Mobilstation MT über entsprechende Eingabebefehle. Dadurch entsteht eine hohe Sicherheit für die Benutzergeräte und die Mobilstationen, die völlig netzunabhängig auf einem zwischen dem Benutzergerät UE und dem in die Mobilstation eingesetzten Identitätsmodul USIM basierenden Verfahren abläuft. Das teilnehmergesteuerte Sperren und Entsperren auf Basis des Benutzergeräts UE mit der der Bindung an das jeweilige Identitätsmodul USIM erlaubt eine serielle Nutzung mehrerer Module in Chipkarten UICC (bzw. SIM-Karten für GSM-Systeme) - in ein- und demselben Benutzergerät, was insbesondere beim Übergang des mobilen Teilnehmers in mehrere Funk-Kommunikationssysteme in Bezug auf die Sicherungsfunktionen von Vorteil ist.

[0018] Mehrere Mechanismen sind zur Implementierung des teilnehmergesteuerten Sperr- und Entsperrvorgangs anwendbar, von denen im folgenden drei Beispiele angegeben sind. Dabei reichen diese Beispiele von einfach bis aufwendig, wobei letztgenannte Ausführungsbeispiele den Vorteil einer höheren Sicherheit bieten.

[0019] Allen Beispielen ist gemeinsam, dass in der Speichereinrichtung MU des Benutzergeräts UE der Zustand LST, eine unveränderbare Gerätekennung IMEI (user equipment identity) und einige zusätzliche Daten gespeichert sind.

[0020] Eine erste Variante - siehe unter 1. in den Figuren 2 bis 4 - zum Sperren/Entsperren besteht darin, in der Speichereinrichtung MU einen unveränderbaren Wert VAL abzulegen, der auch von dem Identitätsmodul USIM gespeichert wird. Falls die Sperre wirkt (lock enabled), sendet das Benutzergerät UE den Wert VAL und die Gerätekennung IMEI in der Nachricht LERQ zum Identitätsmodul USIM, das - nach erfolgreicher Authentifikation - den Wert VAL and die Gerätekennung IMEI in seinem Speicher speichert und die Sperre durch Änderung des Zustands LST' im Modul setzt. Zu einem späteren Zeitpunkt, im Falle der Authentifikation zwischen Benutzergerät UE und Identitätsmodul USIM - siehe FIG 3 - , sendet das Modul den gespeicherten Wert VAL in der Nachricht UARS zum Gerät. Dieser eintreffende Wert VAL wird mit dem in der Speichereinrichtung MU abgelegten Wert VAL verglichen. Die Identifikation des Benutzergeräts UE anhand der Gerätekennung IMEI verhindert, dass der Wert VAL im Modul USIM bei Einsetzen des Moduls USIM in ein anderes Benutzergerät UE überschrieben wird, wobei das Benutzergerät UE, das ursprünglich an dieses Modul gebunden war, unbrauchbar würde. Diese Vorgehensweise erlaubt so viele Benutzergeräte UE an ein einziges Identitätsmodul USIM zu binden, wie Speicherkapazität hierfür im Modul vorhanden ist.

[0021] Eine zweite Variante - siehe unter 2. in den Figuren 2 bis 4 - zum Sperren/Entsperren besteht darin, dass die Speichereinrichtung einen unveränderbaren Schlüssel KEY sowie zwei Sicherungsfunktionen FUN1 und FUN2 enthält. Das Identitätsmodul USIM speichert ebenso in seinem Speicher den Schlüssel KEY, die Gerätekennung IMEI und die beiden Sicherungsfunktionen FUN1 und FUN2. Zum Setzen der Sperre sendet das Benutzergerät UE den Schlüssel KEY und ihre Gerätekennung IMEI in der Nachricht ELRQ zum Modul USIM. Das Modul speichert die eintreffenden Daten KEY und IMEI nach erfolgreicher Teilnehmeraurhentifi-

kation. Zu einem späteren Zeitpunkt, im Falle der Authentifikation zwischen Benutzergerät UE und Identitätsmodul USIM - siehe FIG 3 - , erzeugt das Gerät eine Zufallszahl RND und sendet sie zusammen mit der Kennung IMEI in der Nachricht UARQ zum Modul. Das Modul berechnet anhand der Sicherungsfunktion FUN1, des gespeicherten Schlüsels KEY und der empfangenen Zufallszahl RND eine zugehörige Antwort RES und sendet sie in der Nachricht UARS zum Gerät zurück.

[0022] Bei Eintreffen der Antwort wird von der Steuereinrichtung CU eine zugehörige Antwort RES nach demselben Verfahren berechnet und das Eergebnis mit der vom Modul empfangenen Antwort verglichen.

[0023] Wenn die Sperre im Benutzergerät UE wirkt und das richtige Identitätsmodul USIM eingesetzt ist, kann diese Sperre teilnehmergesteuert aufgehoben werden, indem der Teilnehmer SUB den Befehl LDCM initiiert - siehe FIG 2. In diesem Fall generiert das Benutzergerät UE eine Zufallszahl RND und sendet sie gemeinsam mit der Kennung IMEI in der Nachricht LDRQ zum Modul USIM. Das Modul verifiziert die Kennung IMEI, authentifiziert den Teilnehmer SUB und, falls diese erfolgreich ist, berechnet die Antwort RES unter Anwendung des Schlüssels KEY, der Zahl RND und der Sicherungsfunktion FUN2. Die auf diese Weise berechnete Antwort RES wird zum Gerät UE gesendet, wo sie dessen Entsperren durch Ändern des Zustands LST bewirkt. Vorzugsweise werden immer zwei verschiedene Funktionen FUN1 and FUN2 zum Schutz gegen Attacken benutzt, die vor allem die Modifikation der über die Schnittstelle zwischen Gerät und Modul übertragenen Nachrichten zum Ziel haben. Bei einer einzelnen Sicherungsfunktion könnte die Nachricht LDRQ auf dieser Schnittstelle abgehört, zur Nachricht UARQ modifiziert an das Modul USIM weitergeleitet werden. Danach würde die Antwort vom Modul abgehört werden, ohne dass eine Authentifikation erfolgt, und anschließend eine geeignete Nachricht DLRS zum Gerät UE unter Nutzung der abgehörten Antwort RES gesendet werden.

[0024] Die dritte Variante - siehe unter 3. in den Figuren 2 bis 4 - zum Sperren/Entsperren besteht darin, dass die Speichereinrichtung MU genügend Speicherplatz besitzt, um einen öffentlichen Schlüssel PUK sowie eine Verifizierungsalgorithmus VER zu speichern. Das Modul USIM enthält in seinem Speicher ebenso den öffentlichen Schlüssel PUK, einen dazu korrespondierenden privaten Schlüssel PRK, und eine Unterzeichnenfunktion SIGN (signing function). Nachdem das Gerät UE das Modul USIM zum Entsperren auffordert und der Teilnehmer SUB sich erfolgreich gegenüber dem Modul USIM authentifiziert hat, sendet das Modul USIM ihren öffentlichen Schlüssel PUK. Wenn das Gerät eine Authentifikation durchführt, generiert es eine Zufallszahl RND und sendet sie in der Nachricht UARQ zum Modul. Das Modul berechnet eine Antwort RESP, nutzend die Unterzeichnerfunktion SIG, die Zahl RND und ihren privaten Schlüssel PRK, und sendet das Ergebnis in der Nachricht UARS zum Gerät UE. Das Gerät verifiziert, ob die empfangene Antwort RES eine korrekte Antwort auf die Zufallszahl RND ist, indem sie die Verfizierungsfunktion VER, den öffentlichen Schlüssel PUK des Moduls USIM und die Zahl RND zur Berechnung einer eigenen Antwort benutzt und das Ergebnis mit der empfangenen Antwort RES vergleicht.

[0025] Die zweite Variante schützt vor allem gegen ein Abhören auf der Schnittstelle zwischen Gerät UE und Modul USIM, da der geheime Schlüssel KEY weder das Gerät noch das Modul USIM verläßt, solange nicht die Sperre erstmalig erfolgreich aufgehoben wird, wofür die Authentifikation notwendig ist. as

Patentansprüche

1. Verfahren zur Sicherung von Benutzergeräten (UE) in Mobilstationen (MT) mobiler Teilnehmer eines Funk-Kommunikationssystems, wobei jede Mobilstation (MT) außer dem Benutzergerät (UE) ein Identitätsmodul (USIM) mit teilnehmerbezogenen Daten zur Identifizierung des mobilen Teilnehmers gegenüber dem Funk-Kommunikationssystem aufweist,
   dadurch gekennzeichnet,
   dass das Benutzergerät (UE) durch ein teilnehmergesteuertes Sperren und Entsperren gegen einen Missbrauch gesichert wird.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet,
   dass durch das Sperren und Entsperren des Benutzergeräts (UE) eine Bindung an das Identitätsmodul (USIM) erzeugt und aufgehoben wird.

3. Verfahren nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   dass zum Sperren und Entsperren des Benutzergeräts (UE) eine Teilnehmerauthentifikation gegenüber dem Identitätsmodul (USIM) durchgeführt wird.

4. Verfahren nach Anspruch 3,
   dadurch gekennzeichnet,
   dass für die Teilnehmerauthentifikation andere Sicherheitsparameter (VAL, KEY, PUK, PRK) als die bei einer Benutzerauthentifikation zur Überprüfung der Zugangsberechtigung eines mobilen Teilnehmers zum Funk-Kommunikationssystem benutzten Sicherheitsparameter angewendet werden.

5. Verfahren nach Anspruch 3 oder 4,
   dadurch gekennzeichnet,
   dass zur Teilnehmerauthentifikation eine persönliche Identifikationsnummer (SPIN) verwendet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass beim Sperren und Entsperren des Benutzergeräts (UE) ein privater Schlüssel (PRK) und ein öffentlicher Schlüssel (PUK) als Sicherheitsparameter verwendet werden.

7. Verfahren nach Anspruch 6,
dadurch gekennzeichnet,
dass der öffentliche Schlüssel (PUK) in einer Speichereinrichtung (MU) des Benutzergeräts (UE) und der private Schlüssel (PRK) in dem Identitätsmodul (USIM) abgelegt und von dem Benutzergerät (UE) zur Überprüfung der Identität des Identitätsmoduls (USIM) benutzt werden.

8. Verfahren nach Anspruch 6 oder 7,
dadurch gekennzeichnet,
dass die Identität des Identitätsmoduls (USIM) überprüft wird, indem

- das Benutzergerät (UE) eine Zufallszahl erzeugt und zu dem Identitätsmodul (USIM) sendet,
- das Identitätsmodul (USIM) anhand der Zufallszahl und dem privaten Schlüsel (PRK) eine Antwort (RES) erzeugt und zu dem Benutzergerät (UE) sendet, und
- das Benutzergerät (UE) die empfangene Antwort (RES) mit einer anhand öffentlichen Schlüssels (PUK) berechneten eigenen Antwort verifiziert.

9. Mobilstation (MT) eines mobilen Teilnehmers eines Funk-Kommunikationssystems, mit einem Benutzergerät (UE) und einem Identitätsmodul (USIM) zur Speicherung von teilnehmerbezogenen Daten für eine Identifizierung des mobilen Teilnehmers gegenüber dem Funk-Kommunikationssystem,
dadurch gekennzeichnet,
dass das Benutzergerät (UE) Mittel (CU, MU) zum teilnehmergesteuerten Sperren und Entsperren des Identitätsmoduls (USIM) aufweist.

10. Verfahren nach Anspruch 9,
dadurch gekennzeichnet,
dass Durch die Mittel (CU; MU) zum Sperren und Entsperren des Benutzergeräts (UE) eine Bindung an das Identitätsmodul (USIM) erzeugbar und aufhebbar ist.

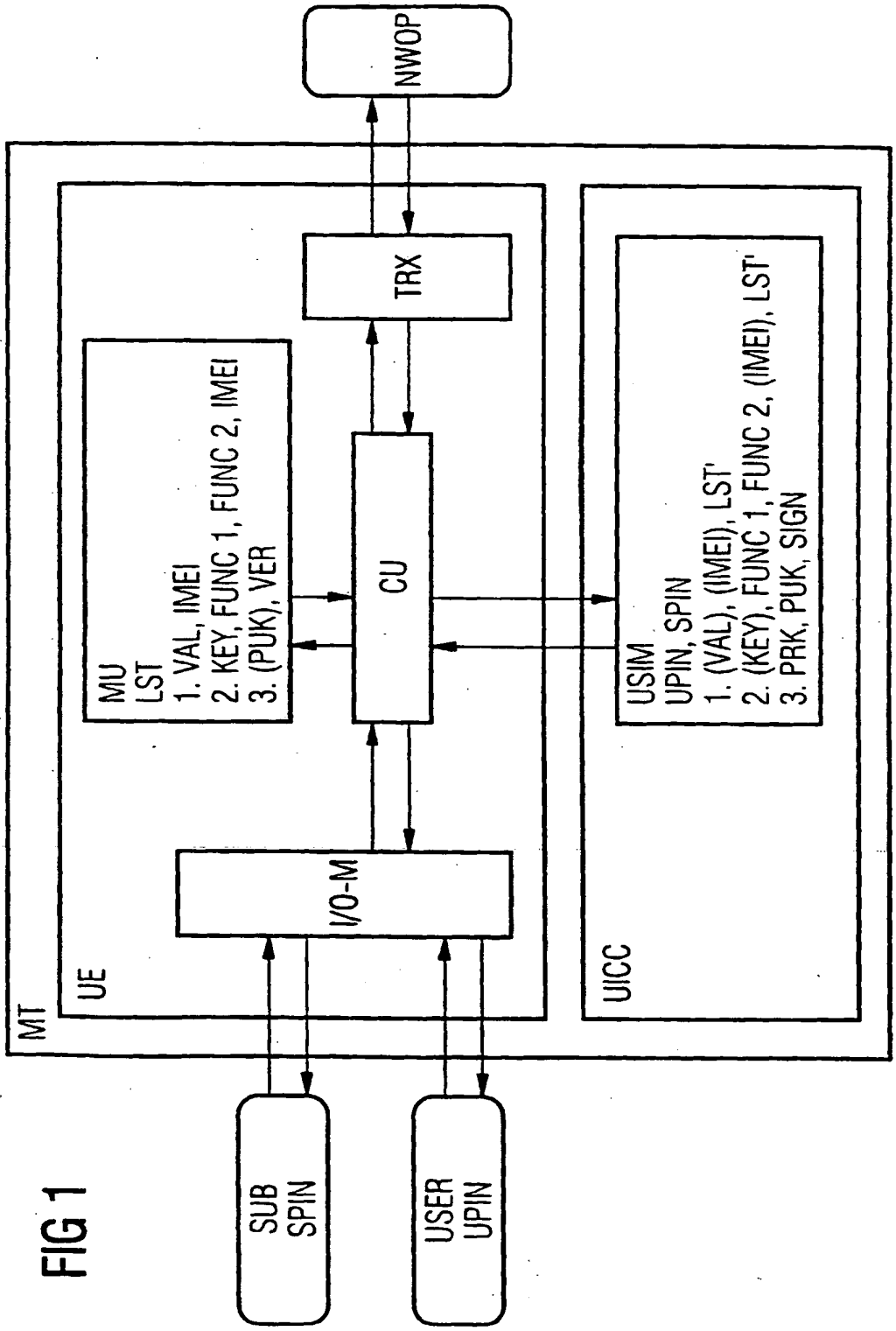


FIG 1

FIG 2

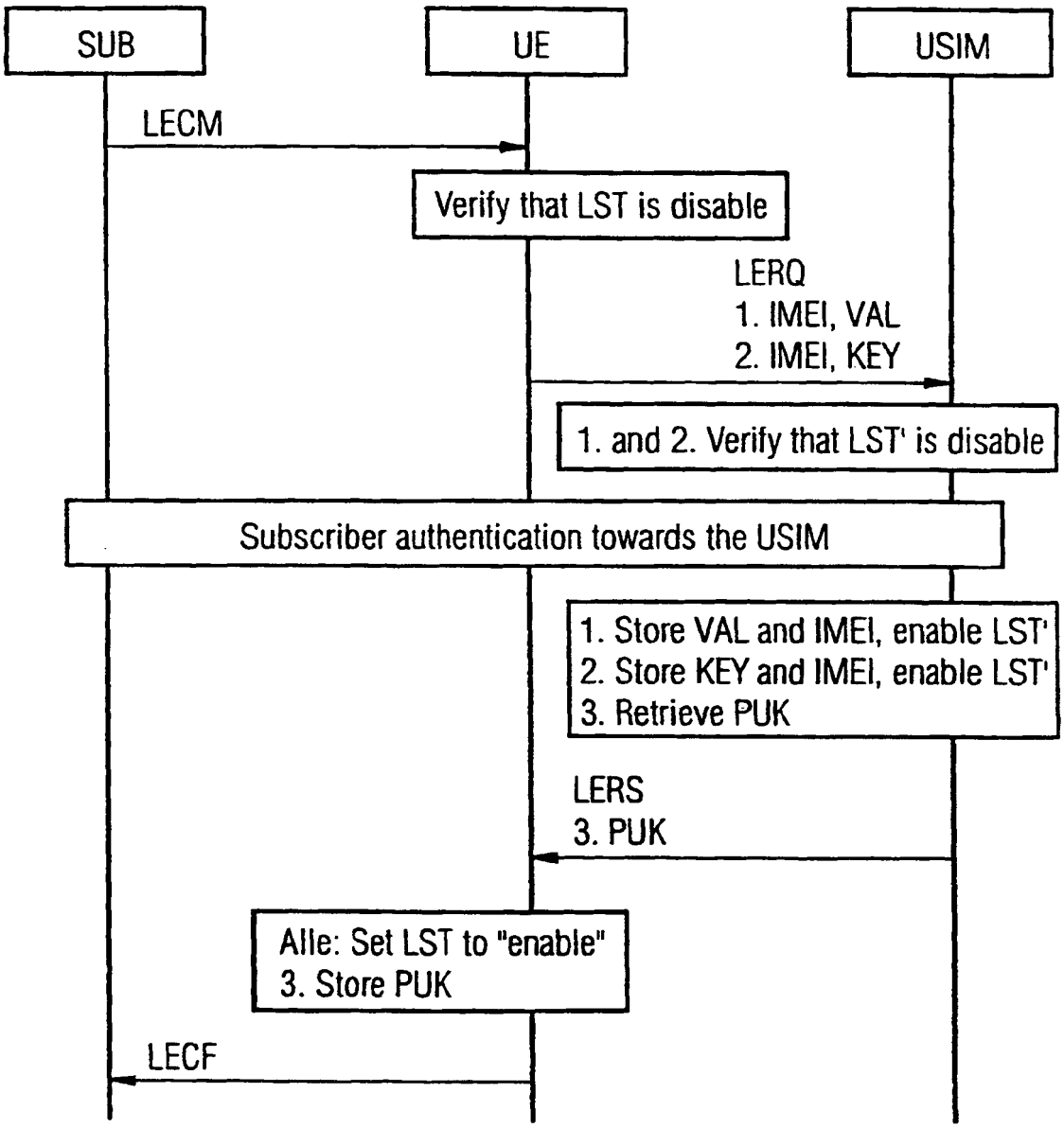


FIG 3

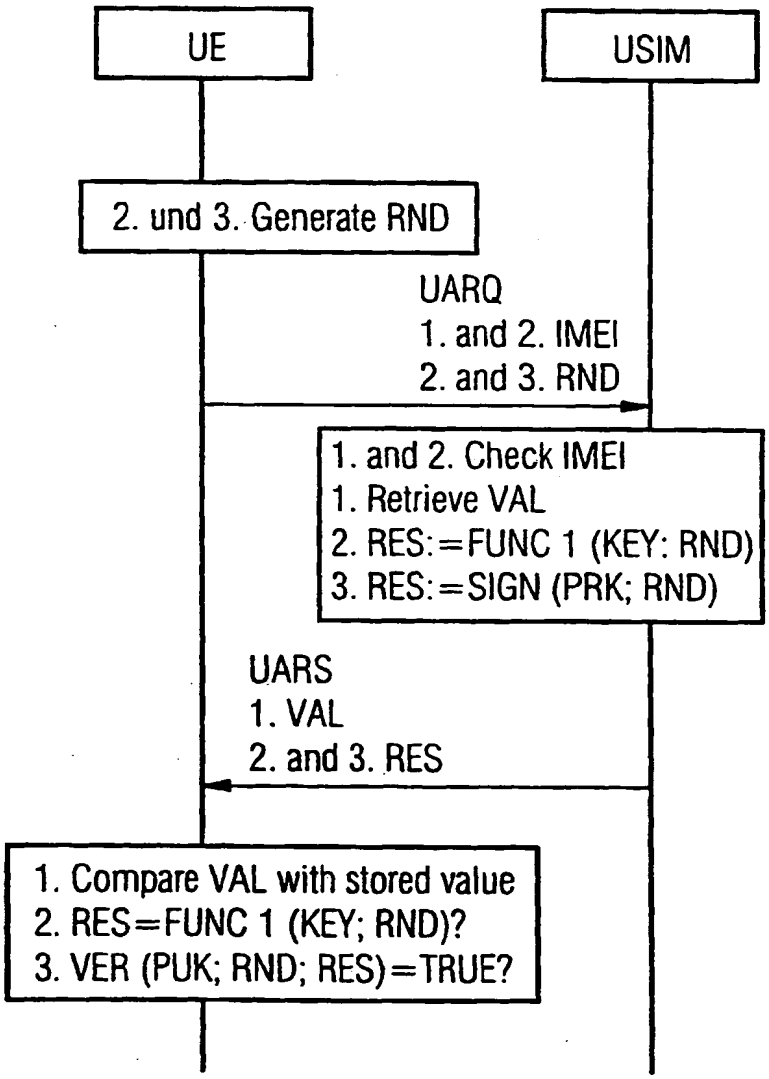
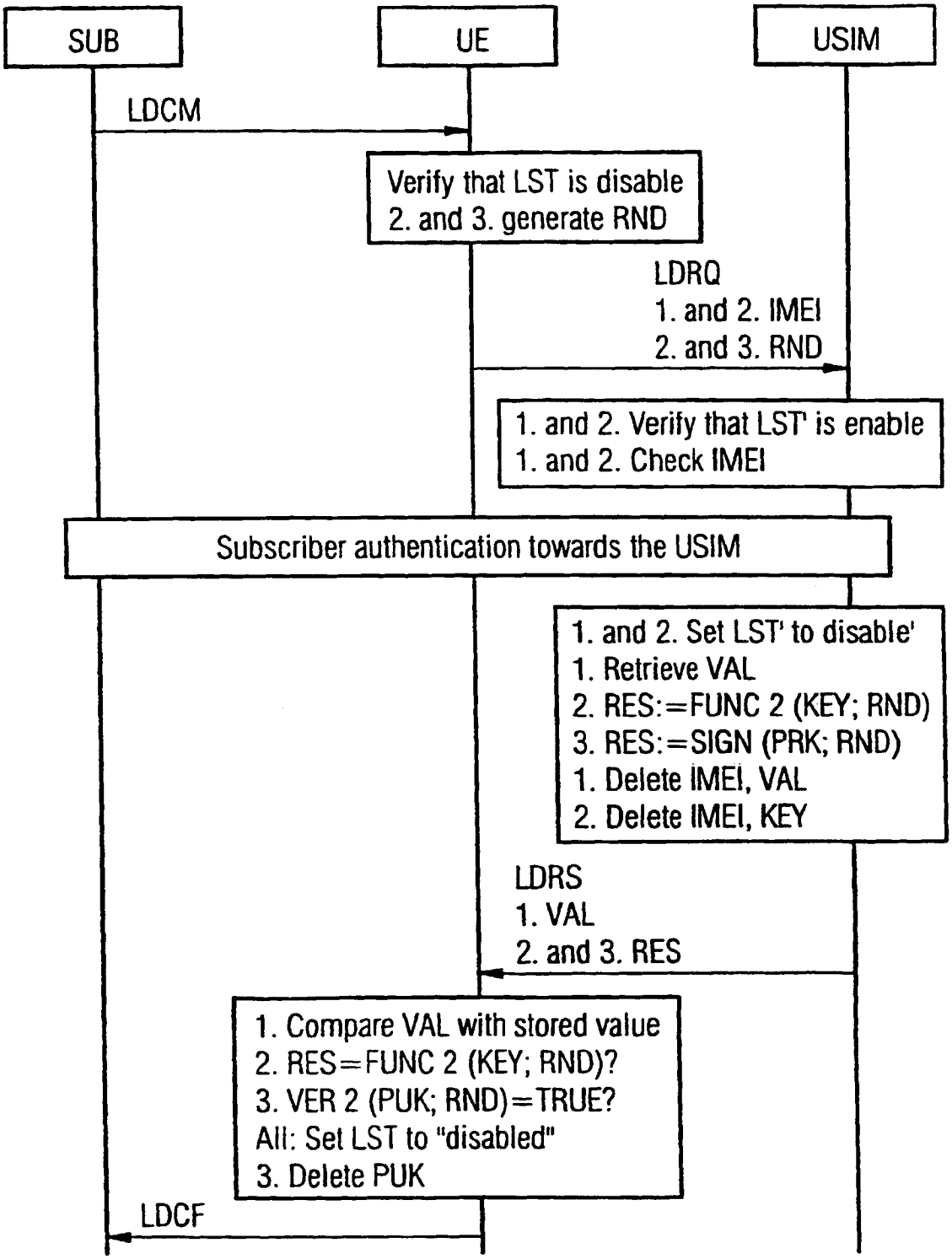


FIG 4



Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 99 12 1688

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	EP 0 750 438 A (NOKIA MOBILE PHONES LTD) 27. Dezember 1996 (1996-12-27) * Spalte 3, Zeile 26 - Spalte 4, Zeile 48 *	1-5,9,10	H04Q7/32
X	DE 92 17 379 U (ERICSSON SE) 29. April 1993 (1993-04-29) * Seite 4, Zeile 27 - Seite 8, Zeile 35 *	1-5,9,10	
X	DE 42 42 151 C (DETECON GMBH) 24. März 1994 (1994-03-24) * das ganze Dokument *	1-5,9,10	
A	DAVIO M ET AL: "METHODOLOGY IN INFORMATION SECURITY. MUTUAL AUTHENTICATION PROCEDURES APPLICATION TO ACCESS CONTROL" INTERNATIONAL ZURICH SEMINAR ON DIGITAL COMMUNICATIONS,CH,ZURICH, I.E.E.E, Bd. PROC. 1982, 1982, Seiten 87-92, XP002014402 * Seite 89, rechte Spalte, Zeile 1 - Seite 92, linke Spalte, Zeile 20 *	1-10	

RECHERCHIERTE SACHGEBIETE (Int.Cl.7)
H04Q

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	7. März 2000	Weinmiller, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 99 12 1688

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

07-03-2000

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0750438 A	27-12-1996	FI 953026 A	20-12-1996
		US 5956633 A	21-09-1999
DE 9217379 U	29-04-1993	SE 470519 B	27-06-1994
		AU 672239 B	26-09-1996
		AU 5049893 A	19-05-1994
		BR 9304655 A	14-06-1994
		CA 2102391 A	10-05-1994
		CN 1091877 A	07-09-1994
		DE 69315419 D	08-01-1998
		DE 69315419 T	20-05-1998
		EP 0607767 A	27-07-1994
		ES 2110078 T	01-02-1998
		FI 934924 A	10-05-1994
		HK 1004924 A	11-12-1998
		JP 6216842 A	05-08-1994
		KR 136247 B	01-06-1998
		MX 9306801 A	31-01-1995
		NZ 248995 A	28-05-1996
		SE 9203351 A	10-05-1994
		SG 49024 A	18-05-1998
		US 5940773 A	17-08-1999
DE 4242151 C	24-03-1994	AT 167608 T	15-07-1998
		DE 59308696 D	23-07-1998
		EP 0602319 A	22-06-1994
		ES 2119838 T	16-10-1998

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82